ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Overview on Minimizing Distortion in Image Steganography

Poonam Talele, Prof. Vanita Mane

ME Computer Student, Department of Computer Engineering, Y.T.C.E.M, Mumbai University, Bhivpuri, Mumbai

Associate Professor, Department of Computer Engineering, RAIT, Mumbai University, Nerul, Mumbai, India

ABSTRACT: A steganography can be widely used in real- world for hiding data under any digital document. A digital document may consist of any audio, video or images. This steganography technique can be useful in various applications such as military for confidential data, University for hiding question papers, in hospital for hiding patient's detail, in smart cards, etc. Since there are several techniques available to achieve steganography such as substitution method, transform domain method, statistical method, distortion method and many more. While using this method several limitations are arises as message difficult to recover, loss of message while image compression, distortion occur while image steganography occur etc. Basically, our paper is based on minimizing distortion in an image. Shuffling, double processing distortion control (DPDC), connectivity preserving, edge line distortion method, these are the methods used for minimizing distortion in image steganography. Basically, our paper is based on connectivity preserving, shuffling and DPDC.

KEYWORDS: Image steganography, Flippability, distortion, shuffling, connectivity preserving, DPDC.

I. Introduction

Steganography is the technique to hide secret information in media so that only sender and receiver can detect information. Since Fig. 1 shows the classification of steganography. Audio steganography is the technique of hiding the secret information into another medium such as audio file. Image steganography hide the message in the image file so that no changes take place after the message insertion in the image file. A text semagram hides a message by updating the look of the carrier text, such as slight changes in font size or type, adding extra spaces, or different additions in letters or handwritten text [1].

Since, there are so many limitations of steganography, such as, message is hard to recover if image is attack such as translation and rotation**.** Major damage to picture exterior,message difficult to recover, relatively easy to detect, image is distorted, message easily lost if picture subject to compression, basically this paper is based on minimizing distortion. As high undetectability of the secret messages can reduce the detection of information from attackers and thus improve the security. To this end, we focus on designing a secure binary image data hiding technique by improving the undetectability while maintaining the stego image equality and embedding capacity i.e. to minimize the distortion present in an image steganography. For this purpose we need to focus on the different techniques of minimizing distortion.

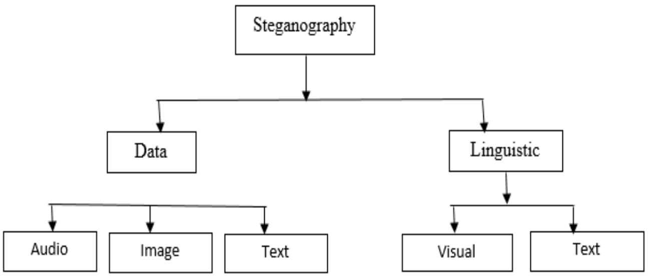

Fig 1. Classification of steganography [1].

DOI: 10.15680/IJIRCCE.2017. 0506133

The remainder of this report is organized as, in section II, we introduce the literature survey of different methods, section III describes methodology to minimize the distortion and last section IV is the conclusion of paper.

II. LITERATURE SURVEY

Flipping pixelson the border may cause a minimum distortion. DRD says that the distortion score is inversely proportional to the distance between the pixel and the border, distance reciprocal distance method (DRD) follow this rule[2]. In shuffling, distortion is measured based on both smoothness and connectivity. It shows that, best flipping location is to be found at the centre of the “l-shape” patternaccording SCD [3].We define an edge line (ELD) as the common sharing line connecting two neighbouring pixelswhere the pixel values for the two pixels are different.Theedge pixel refers to pixels on the edge. ELD suggests that a good flipping location affect the boundary connectivity as little as possible [4].

The “non-intersection” property of the even-even and odd-odd, or even-odd and odd-even processing cases renders the option to merge the two processing cases to minimize the distortion, namely, double processing with distortion control(DPDC).DPDC uses the interlaced morphologicalwavelet transform (IMWT) to embed message bits into theshift edges[5].Through establishing anintense edge-adaptive grid (EAG) along the object contours, we usea simple binary image to show that EAG more economically selects good data carrying pixel locations (DCPL) connected with “l-shaped” patterns than block-based methods [6].To achieve the uniformembedding, the distortion function, to be used,should be designed such that the coefficients having different magnitudes are chosen with a same priority [7].

III. METHODOLOGY

A. *Connectivity preserving method:*

Connectivity along pixels plays an important task to their visual qualities. We resolve two issues one is the “visual distortion” and “uneven embedability”. In this, paper emphasizes the 4- connectivity and 8-connectivity such that better edge pattern will be selected for data hiding. Fliping the pixel will not destroy the connectivity b/w pixels in the neighborhood (VH), does not create extra clusters (IR) and does not destroy the 8-connectivity among pixels(*C*). All these collectively called as “Connectivity-Preserving Criterion”. In this, VH Transition is the number of black or white transition along the vertical or horizontal directions, IR Transition is the number interior right angle transition in 3X3 block and C Transition is the transitions from the center pixel to the sharp corners in 3X3 block. “Flippability Criterion” of center pixel in the 3X3 block is flappable if and only if number of VH transition, IR transition and C transition remain same before and after flipping the center pixels. Fig.2. and Fig.3. shows the authentication and verification process.

Main Objectives

1. Estimate the “flippability” of a pixel using the connectivity-preserving criterion to obtain good visual quality of the watermarked image.
2. Manage the “uneven embedability” of the image by embedding the watermark only in those “embeddable” blocks.
3. Study the different features in flipping pixels in binary images to obtain blind watermark extraction.
4. Search different ways of partitioning the image to achieve larger capacity.

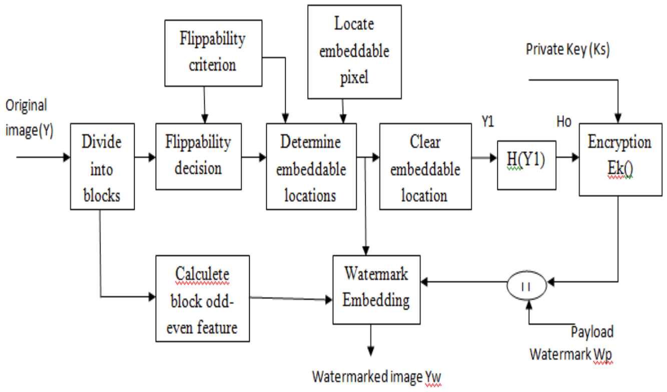

Fig.2. Block diagram of authentication process [8]

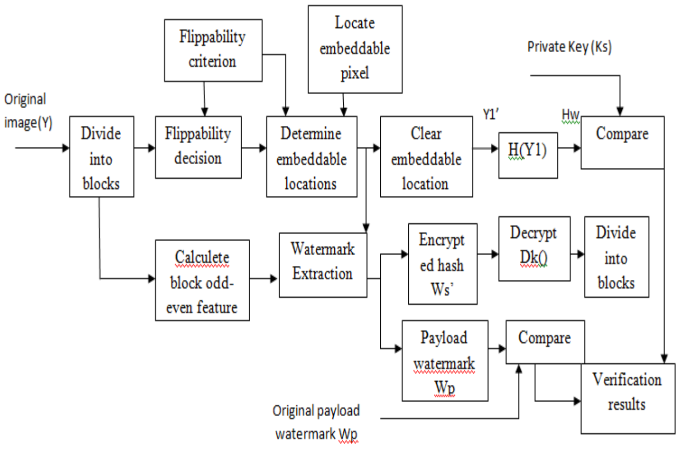

Fig.3. Block Diagram of Verification Process

5. Investigate on how to place the “embeddable” pixels in the watermarked image so as to include cryptographic signature to obtain higher security [8].

B. *Authentication and Annotation based method:*

Shuffling is used before embedding to balance the uneven embedding capacity from region to region. The hidden data from image can be extracted without using the original image, and can also be precisely extracted after high quality printing and scanning with the use of a few registration marks. The proposed data embedding technique is used to detect illegal use of a digitized signature, and annotate or authenticate binary documents. In images, the pixels can take value from only a few possibilities, and hiding data without causing visible distortion becomes more difficult. Basically, flipping white or black pixels that are not on the boundary is likely to establish visible distortion in binary images [3].

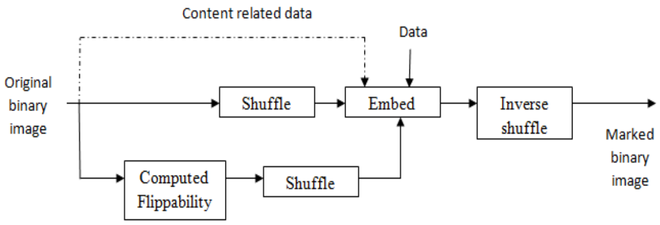

Fig.4. Block diagram of embedding process [3]

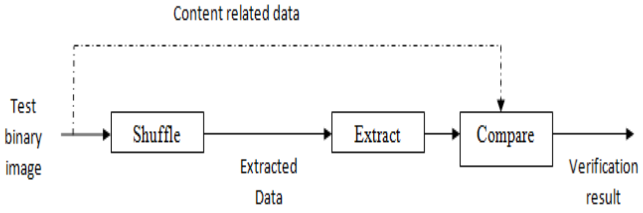

Fig.5. Block diagram of extraction process [3]

C. *MBWT Domain based method:*

The aim of this paper is data hiding for binary images in morphological transform domain. We process the images based on 2X2 pixel blocks and merge two different processing cases that the flippability conditions of one are not affected by flipping the candidates of another for data embedding, namely "orthogonal embedding". We determine the problem of data hiding for binary images in morphological transform domain. Data hiding in real-valued transform domain does not work well for binary images because of the quantization errors introduce in the pre/post- processing [9]. In addition, embedding data using real-valued coefficients requires large memory space. We notice that the morphological binary wavelet transform (MBWT) can be used to track the transitions in binary images by utilizing the detail coefficients [10]. One rather perceptive idea in employing the morphological binary wavelet transform for data hiding is to use the detail coefficients as a location map to determine the data-hiding locations. However, this makes it difficult to get blind watermark extraction due to the reality that once a pixel is flipped; the horizontal, vertical and diagonal coefficients will change likewise. The goal of designing an interlaced transform to recognize the embeddable locations is annoyed by the fact that some transition information is lost during the calculation of a single transform and there is a need to keeptrack of transitions between two and three pixels for binary images data hiding. The "non-intersection" property of the even-even and odd-odd, or even-odd and odd-even processing cases renders the possibility to join the two processing cases to minimize the distortion, namely, double processing with distortion control (DPDC). Embedding data using DPDC is called as orthogonal embedding. The idea of using MBWT for data hiding is to use the coefficients as a location map to define the data hiding locations, since these coefficients hold the edge information in horizontal, vertical and diagonal directions. However, flipping a pixel contains changing the coefficients, as illustrated in Fig.5. It shows that the same edges used to define the data-hiding locations cannot be found in the watermarked image [5].

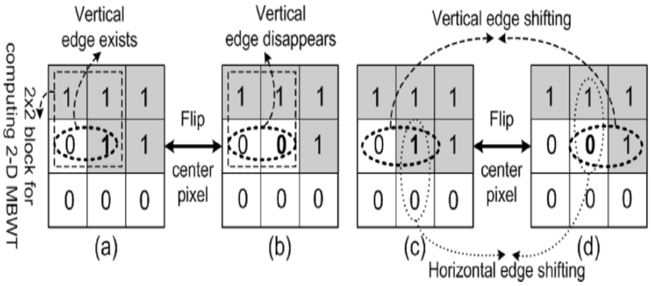

Fig.6. Changes in coefficient due to flipping pixels (a), (b) and shifting off edges (c) and (d) [5]

IV. CONCLUSION

In steganography, after embedding data in an image, it should be protected from attacker. If the distortion present in an image then it can be easily detectable by human vision. The objective of this paper is to minimize the distortion present in stego image by improving image quality and maintaining statistical security. There are several techniques are available to minimize the distortion but my paper is based on Connectivity preserving method, authentication and annotation based method and MBWT based method. From above analysis, as per our knowledge DPDC and Shuffling is the best method as compare to other to achieve steganography with minimum distortion, because of drawbacks of less ELD and DRD score and uniform embedding region.

REFERENCES

1. RonakDoshi, Pratik Jain, Lalit Gupta, "Steganography and its application in security" International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638

2. H. Lu, A. C. Kot, and Y. Q. Shi, "Distance-reciprocal distortion measure for binary document images," *IEEE Signal Process. Lett.*, vol. 11, no. 2,pp. 228–231, Feb. 2004.I.S. Jacobs and C.P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

3. H. Lu, A. C. Kot, and Y. Q. Shi, "Distance-reciprocal distortion measure for binary document images," *IEEE Signal Process. Lett.*,vol. 11, no. 2,pp. 228–231, Feb. 2004.R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

4. J. Cheng and A. C. Kot, “Objective distortion measure for binary text image based on edge line segment similarity,” *IEEE Trans. Image Process.*, vol. 16, no. 6, pp. 1691–1695, Jun. 2007.

5. H. Yang, A. C. Kot, and S. Rahardja, “Orthogonal data embedding for binary images in morphological transform domain—A high-capacity approach,” *IEEE Trans. Multimedia*, vol. 10, no. 3, pp. 339–351, Apr. 2008.

6. H. Cao and A. C. Kot, “On establishing edge adaptive grid for bilevel image data hiding,” IEEE Trans.Inf. Forensics Security, vol. 8, no. 9,pp. 1508–1518

7. Fangjun Huang and Jiwu Huang “Distortion Function Designing for JPEG Steganography with Uncompressed Side-image”

8. H. Yang and A. C. Kot, “Pattern-based data hiding for binary image authentication by connectivity-preserving,”*IEEE Trans. Multimedia*, vol. 9, no. 3, pp. 475–486, Apr. 2007

9. Q. G. Mei, E. K. Wong, and N. D. Memon, “Data hiding in binary text documents,” *Proc. SPIE*, vol. 4314, pp. 369–375, Aug. 2001.

10. P. W. Wong and N. Memon, “Secret and public key image watermarking schemes for image authentication and ownership verification”, Polytechnic University, Brooklyn, NY 11201

BIOGRAPHY

Poonam Janardan Taleleis a ME Research Student in the Computer Engineering Department, Yadavrao Tasgaonkar College of Engineering and Management (Y.T.C.E.M), Bhivpuri, Mumbai,Mumbai University. She received Bachelor of Engineering (BE-Computer) degree in 2008 from SSJCOE, Mumbai, MS, India. Her research interests are Computer Security, Algorithms, Artificial Intteligence etc.